526 Rec'd PCT/PTO 18 JUL 2001

FORM PTO-1390 (Modified) (REV 11-98) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: **09669/004001**

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR): **09/889524**

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR00/00099	**18 January 2000**	**18 January 1999**

TITLE OF INVENTION

METHOD FOR SECURE DOWNLOADING OF DATA BETWEEN SECURITY UNITS

APPLICANT(S) FOR DO/EO/US

Dan BUTNARU and Raphaël ROSSET

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ A copy of the International Search Report (PCT/ISA/210).
8. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
9. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
11. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☒ Certificate of Mailing by Express Mail
20. ☒ Other items or information:

22511

PATENT TRADEMARK OFFICE

A copy of the French Search Report

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR) 09/889524	INTERNATIONAL APPLICATION NO. PCT/FR00/00099	ATTORNEY'S DOCKET NUMBER 09669/004001

21. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :		CALCULATIONS PTO USE ONLY
☐ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO and International Search Report not prepared by the EPO or JPO	$970.00	
☒ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but Internation Search Report prepared by the EPO or JPO	$840.00	
☐ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	$690.00	
☐ International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4)	$670.00	
☐ International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4)	$96.00	
ENTER APPROPRIATE BASIC FEE AMOUNT =		$840.00
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).		$0.00

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	20 - 20 =	0	x $18.00	$0.00
Independent claims	1 - 3 =	0	x $78.00	$0.00
Multiple Dependent Claims **(check if applicable).**			☒	$260.00
TOTAL OF ABOVE CALCULATIONS			=	$1,100.00
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) **(check if applicable).**			☐	$0.00
SUBTOTAL			=	$1,100.00
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)).			+	$0.00
TOTAL NATIONAL FEE			=	$1,100.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).**			☐	$0.00
TOTAL FEES ENCLOSED			=	$1,100.00
			Amount to be: refunded	$
			charged	$

☒ A check in the amount of **$1,100.00** to cover the above fees is enclosed.

☐ Please charge my Deposit Account No. in the amount of to cover the above fees.
A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **500-591** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

ROSENTHAL & OSHA L.L.P.
700 Louisiana, Suite 4550
Houston, Texas 77002

Telephone: (713) 228-8600
Facsimile: (713) 228-8778

SIGNATURE

Jonathan P. Osha
NAME

33,986
REGISTRATION NUMBER

7/17/01
DATE

JC18 Rec'd PCT/PTO 18 JUL 2001
09/889524

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10) Applicant(s): **Dan BUTNARU et al.**	Docket No. **09665/004001**

Serial No.	Filing Date	Examiner	Group Art Unit
	July 18, 2001		

Invention: **METHOD FOR SECURE DOWNLOADING OF DATA BETWEEN SECURITY UNITS**

I hereby certify that the following correspondence:

PCT National Phase Application

(Identify type of correspondence)

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to: The Assistant Commissioner for Patents, Washington, D.C. 20231 on

July 18, 2001
(Date)

Rhonda L. Parker
(Typed or Printed Name of Person Mailing Correspondence)

(Signature of Person Mailing Correspondence)

EL656798225US
("Express Mail" Mailing Label Number)

Note: Each paper must have its own certificate of mailing.

EL656798225US

09/889524
JC18 Rec'd PCT/PTO 18 JUL 2001

ATTORNEY DOCKET NO. 09669/004001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Dan BUTNARU et al.	Art Unit:	
Serial No.:		Examiner:	
Filed:	July 17, 2001		
Title:	METHOD FOR SECURE DOWNLOADING OF DATA BETWEEN SECURITY UNITS		

Assistant Commissioner for Patent
Washington, DC 20231

PRELIMINARY AMENDMENT

Dear Sirs:

Prior to examination, please amend the application as follows:

IN THE SPECIFICATION

Page 1, between line 5 and line 6, insert: -- FIELD OF THE INVENTION--;

Page 1 between line 25 and line 26, insert: --BACKGROUND OF THE INVENTION--;

Page 2, between line 23 and line 24, insert: --SUMMARY OF THE INVENTION--;

Page 4, between line 2 and line 3, insert: --BRIEF DESCRIPTION OF THE DRAWINGS--; and

Page 4, between line 17 and line 18, insert: --DETAILED DESCRIPTION--.

REMARKS

Full examination and favorable action are requested.

Date of Deposit July 18, 2001
I hereby ~~certify under 37 CFR 1.8(a)~~ that this correspondence is being deposited with the United States Postal Service as **first class mail** with sufficient postage on the date indicated above and is addressed to the Assistant ~~Commissioner for Patents~~, Washington, D.C. 20231

Rhonda L. Parker

RHONDA L. PARKER

Please charge any fees, or make any credits, to Deposit Account No. 500-591,

Reference No. 09669/004001.

Date: 7/17/01

Jonathan P. Osha
Reg. No. 33,986

Rosenthal & Osha L.L.P.
700 Louisiana Street, Suite 4550
Houston, TX 77002

Telephone: 713/228-8600
Facsimile: 713/228-8778

17966_1.DOC

526 Rec'd PCT/PTO 18 JUL 2001
09/889524

PATENT
ATTORNEY DOCKET NO. 09669/004001

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: **METHOD FOR SECURE DOWNLOADING OF DATA BETWEEN SECURITY UNITS**

APPLICANTS: **Dan BUTNARU and Raphaël ROSSET**

"EXPRESS MAIL" Mailing Label Number: EL656798225US
Date of Deposit: July 17, 2001

22511
PATENT TRADEMARK OFFICE

Rec'd PCT/PTO 13 AUG 2001

#3

09/889524

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Dan BUTNARU et al. Art Unit :
Serial No.: 09/889524 Examiner :
Filed : July 18, 2001
Title : METHOD FOR SECURE DOWNLOADING DATA BETWEEN SECURITY UNITS

Assistant Commissioner for Patents
Washington, DC 20231

PRELIMINARY AMENDMENT

Dear Sir:

Before examining the referenced application on the merits, please amend the application as outlined below:

IN THE CLAIMS

Please amend the claims as outlined below. A marked-up version of the claims, illustrating the changes, is attached as Appendix A.

Please cancel claim 1.

Please add the following claims:

--20. (New) A method for customizing a set of several second security units, comprising:

secure downloading of an application key from a first security unit of a central processing unit to said set of second security units, said first unit and second units each comprising at least one memory, wherein the method further comprises for each second unit in said set:

on each downloading, computing an operation key in the first unit based on information specific to the second unit, a transport key, and a diversification algorithm, said transport key residing within the memory of the first security unit, said memory being non volatile;

encrypting the application key in the first unit based on information comprising said operation key and an encryption algorithm;

sending data comprising the encrypted application key to the second unit;

on each downloading, computing an operation key in the second unit based on information specific to the second unit, the transport key and the diversification algorithm, the same transport key residing in the non-volatile memory of each second security unit of said set, said operation key not being stored within the memory of said second unit; and

decrypting the encrypted application key in the second unit based on information comprising said operation key and a decryption algorithm which is the inverse of the encryption algorithm.

21. (New) A method according to claim 3, further comprising:

sending the random information, information pertaining to an application key and information specific to the second unit to the first unit by means of a first single command.

22. (New) A method according to claim 4, further comprising:

sending the random information, information pertaining to an application key and information specific to the second unit to the first unit by means of a first single command.

23. (New) A method according to claim 2, further comprising:

sending the encrypted application key and the information pertaining to an application key to the second unit by means of a single second command.--

Please amend the claims as follows:

2. (Once Amended) A method according to claim 20, further comprising:

sending information specific to the second unit to the first unit before computing the application key in the first unit.

3. (Once Amended) A method according to claim 20, further comprising:

sending a random number provided by the second unit to the first unit, before encrypting the application key in the first unit.

4. (Once Amended) A method according to claim 20, further comprising:

sending information pertaining to an application key to the first unit, before encrypting the application key within said first unit.

5. (Once Amended) A method according to claim 4, further comprising:

choosing the application key to be encrypted based on said information.

6. (Once Amended) A method according to claim 20, wherein said encryption of an application key intended for a second unit is unique.

7. (Once Amended) A method according to claim 20, further comprising:

verifying integrity of the data includes the encrypted application key.

8. (Once Amended) A method according to claim 20, further comprising:

sending information pertaining to an application key to the second unit, before decrypting the encrypted application key within said second unit of said set.

9. (Once Amended) A method according to claim 20, further comprising:

storing within the second unit, after decrypting the encrypted application key, said key within said second unit.

10. (Once Amended) A method according to claim 9, wherein storing of the application key within the second unit is done based on information pertaining to an application key.

11. (Once Amended) A method according to claim 20, further comprising:

verifying that the application key is authentic.

12. (Once Amended) A method according to claim 20, wherein the first security unit comprises a smart card.

13. (Once Amended) A method according to claim 20, wherein the memory comprises a rewritable memory.

14. (Once Amended) A method according to claim 20, wherein a second unit comprises several application keys.

15. (Once Amended) A method according to claim 20, wherein the first unit comprises several application keys.

16. (Once Amended) A method according to claim 20, further comprising:

after encrypting the application key, erasing the operation key temporarily saved within the second volatile memory of the first unit.

17. (Once Amended) A method according to claim 20, further comprising:

after decrypting the application key, erasing the operation key temporarily saved within a second volatile memory in the first unit.

18. (Once Amended) A method according to claim 2, further comprising:

sending the random information, information pertaining to an application key and information specific to the second unit to the first unit by means of a first single command.

19. (Once Amended) A method according to claim 20, further comprising:

sending the encrypted application key and the information pertaining to an application key to the second unit by means of a single second command.

Remarks

The amendments have been made in order to comply with the formal requirements of the USPTO. No new matter was introduced by such amendments, and no amendments were made for reasons relating to patentability. Favorable consideration of this application is respectfully requested.

Please apply any charges not covered, or any credits, to Deposit Account 500-591 (Reference No. 9669.004001).

Respectfully submitted,

Date: 4/8/01

Jonathan P. Osha, Reg. No. 33,986
Rosenthal & Osha L.L.P.
700 Louisiana, Suite 4550
Houston, TX 77002

Telephone: (713) 228-8600
Facsimile: (713) 228-8778

18622_1.DOC

APPENDIX A – MARKED-UP VERSION OF THE CLAIMS

Newly added matter has been indicated by underline, while matter to be appears in brackets and boldface.

2. (Once Amended) A method according to claim **[1]** 20, **[characterized in that it further comprises an additional step of]** further comprising:

[-] sending information specific to the second unit **[(EI)]** to the first unit **[(AS)]** before computing the application key **[(T1)]** in the first unit **[(AS)]**.

3. (Once Amended) A method according to **[claims 1 or 2]** claim 20, **[characterized in that it further comprises an additional step of]** further comprising:

[-] sending a random number provided by the second unit **[(EI)]** to the first unit **[(AS)]**, before encrypting the application key **[(TA)]** in the first unit **[(AS)]**.

4. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises an additional step of]** according to claim 20, further comprising:

[-] sending information pertaining to an application key **[(TA)]** to the first unit **[(AS)]**, before encrypting the application key **[(TA)]** within said first unit **[(AS)]**.

5. (Once Amended) A method according to claim 4, **[characterized in that it further comprises an additional step of]** further comprising:

[-] choosing the application key **[(TA)]** to be encrypted based on said information.

6. (Once Amended) A method **[according to any of the preceding claims, characterized in that]** according to claim 20, wherein said encryption of an application key **[(TA)]** intended for a second unit **[(EI)]** is unique.

7. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises and additional step of]** according to claim 20, further comprising:

[-] verifying integrity of the data **[(DATA)]** includes the encrypted application key **[(TA)]**.

8. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises an additional step of]** according to claim 20, further comprising:

[-] sending information pertaining to an application key **[(TA)]** to the second unit **[(EI)]**, before decrypting the encrypted application key **[(TA)]** within said second unit **[(EI)]** of said set **[(S)]**.

9. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises an additional step of]** according to claim 20, further comprising:

[-] storing within the second unit **[(EI)]**, after decrypting the encrypted application key **[(TA)]**, said key **[(TA)]** within said second unit **[(EI)]**.

10. (Once Amended) A method according to claim 9, **[characterized in that]** wherein storing of the application key **[(TA)]** within the second unit **[(EI)]** is done based on information pertaining to an application key **[(TA)]**.

11. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises an addition step of]** according to claim 20, further comprising:

[-] verifying that the application key **[(TA)]** is authentic.

12. (Once Amended) A method **[according to any of the preceding claims, characterized in that]** according to claim 20, wherein the first security unit **[(AS) is]** comprises a smart card.

13. (Once Amended) A method **[according to any of the preceding claims, characterized in that]** according to claim 20, wherein the memory **[(M) is]** comprises a rewritable memory.

14. (Once Amended) A method **[according to any of the preceding claims, characterized in that]** according to claim 20, wherein a second unit **[(EI)]** comprises several application keys **[(TA)]**.

15. (Once Amended) A method **[according to any of the preceding claims, characterized in that]** according to claim 20, wherein the first unit **[(AS)]** comprises several application keys **[(TA)]**.

16. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises an additional step of]** according to claim 20, further comprising:

[-] after encrypting the application key **[(TA)]**, erasing the operation key **[(T1)]** temporarily saved within the second volatile memory of the first unit **[(AS)]**.

17. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises an additional step of]** according to claim 20, further comprising:

[-] after decrypting the application key **[(TA)]**, erasing the operation key **[(T1)]** temporarily saved within a second volatile memory **[(M2)]** in the first unit **[(EI)]**.

18. (Once Amended) A method **[according to preceding claims 2 to 4, characterized in that it further comprises an additional step of]** according to claim 2, further comprising:

[-] sending the random information, information **[(REF1)]** pertaining to an application key **[(TA)]** and information **[(SN)]** specific to the second unit **[(EI)]** to the first unit **[(AS)]** by means of a first single command **[(EXPORTKEY)]**.

19. (Once Amended) A method [according to preceding claims 1 and 2, characterized in that it further comprises the additional steps of] according to claim 20, further comprising:

[-] sending the encrypted application key [(TA)] and the information [(REF2)] pertaining to an application key [(TA)] to the second unit [(EI)] by means of a single second command [(IMPORTKEY)].

Rec'd PCT/PTO 13 AUG 2001
09/889524

CERTIFICATE OF MAILING BY FIRST CLASS MAIL (37 CFR 1.8) Applicant(s): **Dan BUTNARU et al.**			Docket No. **09669/004001**
Serial No. **09/889,524**	Filing Date **July 18, 2001**	Examiner	Group Art Unit

Invention:

METHOD FOR SECURE DOWNLOADING DATA BETWEEN SECURITY UNITS

I hereby certify that this **Preliminary Amendment**
(Identify type of correspondence)

is being deposited with the United States Postal Service as first class mail in an envelope addressed to: The Assistant Commissioner for Patents, Washington, D.C. 20231 on **August 8, 2001**
(Date)

Rhonda L. Parker
(Typed or Printed Name of Person Mailing Correspondence)

(Signature of Person Mailing Correspondence)

Note: Each paper must have its own certificate of mailing.

EXPRESS MAIL NO. EL 992 762 135 US

09/889524
JC18 Rec'd PCT/PTO 18 JUL 2001

METHOD FOR SECURE DOWNLOADING OF DATA BETWEEN SECURITY UNITS

The present invention relates to a method for customizing a set of several second security units, comprising secure downloading of an application key from a first security unit to said second security units in said set, wherein said first unit and said second units each comprise at least one memory.

In particular, this invention can advantageously be applied during a phase when second security units are customized in such fields as customer fidelity and banking.

Such a customization method is carried out before said second units are put into use. For example, when they are used in the field of customer fidelity, the second units are found in gas station terminals and are used so as to provide security services in debit-credit transactions of fidelity points between one of said terminals and user credit cards. In the banking field, the second units are found in banking terminals and provide secure services for money transactions in user credit cards.

A well-known state of the art which is disclosed in the published US patent No 5 517 667 under the name of DAQ Electronics, teaches that there exists a key encryption system exists for making secure communications that can be established between a second security unit or "master unit" and a third user unit or "remote unit", when the latter is installed in a remote location, such as a portable telephone. This security system is based on the use of a temporary communication key. According to this system, after the user unit has been installed at its remote location, a communication key is generated by means of the second unit. Accordingly, for establishing each communication from

the second unit to the user unit, the encrypted communication key is sent. The communication key enables exchange of secure messages between the second and user units, as it is only known by these two units. More specifically, the key is based on a pair of secret numbers which are unique to each user unit, and the second unit includes all pairs corresponding to all user units. This system is even more secure as a pair of two secret numbers is written within the user unit's memory, which is volatile. Thus, when a communication is completed and when the user unit is no longer supplied with power, this pair is erased and there is no risk of unauthorized discovery of both secret numbers. In order to establish another communication, the system generates another communication key.

The above-mentioned document describes a system which is put into operation when using a second unit and a user unit with an aim to establish a secure communication between both units by using the same communication key, which is dedicated to communications. It provides no description whatsoever of a customization system for secure key downloading in a set of several second security units.

Therefore, a technical problem to be solved by an object of the present invention is to provide a method for customizing a set of several second security units comprising secure downloading of an application key from a first security unit to said second security units in said set, wherein said first unit and second units each comprise at least one memory, so as to prevent, on the one hand, unauthorized discovery of said application key, and on the other hand, to speed up the customization phase of said second security units.

A solution to the technical problem posed is characterized in that said customization method comprises the steps of :

for each second unit in said set,

- on each downloading, computing, in the first unit, an operation key based on a piece of information specific to the second unit, a transport key, and a diversification algorithm, said transport key residing in the memory of the first security unit, said memory being non-volatile,

- encrypting the application key in the first unit, based on information comprising said operation key and an encryption algorithm, said application key residing in said memory,

- sending data comprising the encrypted application key to the second unit,

- on each downloading, computing, in the second unit, the operation key based on the piece of information specific to the second unit, the transport key and the diversification algorithm, wherein the same transport key resides in the non-volatile memory of each second security unit in said set, said operation key not being stored in the memory of said second unit,

- decrypting the encrypted application key in the second unit based on information comprising said operation key and a decryption algorithm which is the inverse of the encryption algorithm.

Therefore, as will be seen in detail below, the downloading method of the present invention enables, by computing said operation key and only preserving it for the period when the application key is being encrypted or decrypted, to improve downloading security of an application key. Therefore, a defrauder will neither be able to access said operation key nor, as a consequence, the application key. Possible tampering is therefore prevented and time-consuming operations for the customization phase are no longer carried out, since the computation time of the operation key is negligible with respect to the access time required for storing said key.

The present invention will be understood more fully from the description given herebelow and from the

accompanying drawings which should not be taken to be limiting the invention.

Figure 1 is a view showing a first unit and several second units belonging to the same set.

Figure 2 is a view showing a first unit and a second unit of Figure 1.

Figure 3 is a view showing a data interchange between the first unit and the second unit of Figure 2.

Figure 4 is a view showing a second interchange of data between the first unit and the second unit of Figure 2.

Figure 5 is a view showing a first interchange of data between the first unit and the second unit of Figure 2.

Figure 6 is a view showing a first interchange of data between the first unit and the second unit of Figure 2.

Figure 1 shows a first security unit AS and several security units EI belonging to the same set S (not shown), each of the units (AS, EI) comprising at least one non-volatile memory M. The first unit AS as well as the second units EI of said set S have the same transport key T and the same algorithm ALGO1, referred to as a diversification algorithm, which reside in memory M. Figure 2 shows unit AS as well as one unit EI from the set S. Each second unit EI of set S has the same transport key T. Thus, a set of second units EI is differentiated from another set by means of transport key T. For example, two sets of second units EI correspond to two different gas station providers.

Moreover, the first unit AS has an application key TA and an encryption algorithm ALGO2. It should be noted that both algorithms ALGO1 and ALGO2 may use the same basic algorithm. Each unit EI of said set S comprises specific information SN and at least one user application (not shown) such as an application providing security services for fidelity point debit-credit transactions.

In order to use security units EI of said set S, each second unit EI of said set S must first download an application key TA from the first unit AS, during a so-called customization phase comprising the steps described below. This key is transferred by means of a standard communications network. A defrauder who would spy on said network or said units is prevented from accessing keys in the units as described below.

In a first step, on each downloading, a computation is made in the first unit AS of an operation key T1 based on the information SN specific to second unit EI, transport key T and diversification algorithm ALGO1, said transport key T residing in memory M of first security unit AS, which memory is non-volatile. Preferably, memory M is a rewritable memory. It should be noted that transport key T remains valid even during the phases when the second unit EI is being used, as long as it is not replaced.

Information SN specific to second unit EI does not reside in the first unit. Therefore, as shown in Figure 3, information SN specific to second unit EI is sent to first unit AS before operation key T1 is computed in first unit AS. First unit AS preferably contains several application keys TA. Said key T1 will serve for downloading one of the application key TA contained in first unit AS, and the selected application key will be encrypted and sent to unit EI. One application key is associated with one user application. The appropriate key is chosen according to the application residing in second unit EI.

As shown in Figure 3, for selecting one of said application keys TA, in a second step, a piece of information REF1 relative to application key TA is sent to first unit AS before encrypting application key TA in said unit AS, and the application key TA to be encrypted is chosen based on said information REF1. For example, a reference representing a key number of three can be sent by second unit EI to indicate that the third key, which

corresponds to an application in said unit EI, has been chosen. It is the latter that will be downloaded into second unit EI. If there is no application key TA referred to by said number REF1, the first unit AS indicates that the key does not exist.

In a third step, as shown in Figure 3, application key TA is encrypted in first unit AS from information comprising said operation key T1 and encryption algorithm ALGO2. The operation key temporarily resides in a second volatile memory (not shown) in first unit AS.

In order to protect first unit AS against possible tampering, after application key Ta has been encrypted, the operation key T1 that was temporarily saved within the second volatile memory of first unit AS is erased.

After said key TA has been encrypted, data "DATA" comprising the encrypted application key TA is sent to the second unit TA.

In a fourth step, encrypted application key TA is decrypted in second unit EI based on information including operation key T1 and a decryption algorithm ALGO2P which is the inverse of encryption algorithm ALGO2. In this step, in order to find out the chosen application key TA, it is necessary to use the same operation key T1 as used for encrypting said application key TA in the first security unit AS. For that purpose, before decrypting said encrypted application key TA, on each download, a computation is made in second unit E1 of operation key T1 based on information SN specific to second unit EI, transport key T and diversification algorithm ALGO1, said same transport key T residing in non-volatile memory M of each second security unit EI of said set S, said operation key T1 not being stored within memory M of a second unit EI. Preferably, the memory M of the second unit is rewritable. The operation key T1 is temporarily saved within a second volatile memory (not shown) in second unit EI.

It should be noted that this computation can be done at any time before application key TA is encrypted. The data items required for computing operation key T1 in second security unit EI are the same as those used for computing operation key T1 in first unit AS. Therefore, both keys T1 are identical and the chosen application key TA is indeed found in second unit EI. It was not necessary to send the operation key T1 over the communication network.

In a fifth step, after application key TA has been decrypted and preferably just before this decryption, the temporarily saved operation key T1 is erased from said second volatile memory in second unit EI.

The fact of, on the one hand, not sending any operation key T1 over the communication network and on the other hand, not storing any operation key T1 within a non-volatile memory M in a second module EI and finally, the fact that said operation key only resides in the second unit only for the time required for decrypting application key TA, makes tampering more difficult to carry out inasmuch as, if a defrauder wishes to find an application key TA, he or she should first find the operation key T1 in use. Finally, this facilitates customization and setting up an n-th second unit EI since, for customizing second units, it is no longer required to carry out two downloads, first one for downloading an operation key TA and second, for downloading an application key TA, but downloading only an application key TA is sufficient. Thus, one gets rid of the first downloading operation which is usually carried out by an entity different from first unit AS, which generally complicates things correspondingly.

Just as the first unit AS, a unit EI will preferably comprise several application keys TA. Thus, by means of a second unit EI, several applications can be handled. Moreover, this improves the security of said units since, on the one hand, it will be more difficult for a defrauder to uncover an application key from among

others, and on the other hand, to know to what application it is dedicated to. In the previous example relating to the field of customer fidelity, when using a second unit EI, the latter should be able to provide various services such as securing debit-credit transactions of fidelity points, for example, for different fuel types. Thus, it is important to have different application key TA in unit EI for managing the security of said different transaction types, which represent different applications.

Therefore, in a sixth step, a piece of information REF2 pertaining to an application key TA is sent to second unit EI before said encrypted application key TA is decrypted in unit EI, as shown in Figure 4. Information REF2 enables to either choose application key TA, which will be assigned the value of the application key originating from the first unit AS, or indicate a location where said key TA provided by said first unit AS will be loaded. Therefore, it is possible to either modify a value of a key TA already residing in said second unit EI, or to download a new application key TA into a second unit EI for a new user application.

In case application key TA referred to by said information REF2 does not exist or said location does not exist or is not designed for accepting a key, second unit EI rejects the received key and indicates that an error has occurred. It should be noted that the REF1 and REF2 information sent to the first and second security units, respectively, can be equivalent.

Later on, when used, one of the application keys TA residing in second unit EI can be used by said unit for identifying itself with respect to external entities such as a user card. However, said identification has to be unique. Therefore, key TA should not have any duplicate. Thus, when it is desired to download this key, the chosen application key TA is diversified within unit AS, before said key is encrypted. Diversification

is done as a function of information specific to each second unit.

Finally, in a last step, after said encrypted application key TA has been decrypted, key TA is stored into second unit EI. Storing application key TA in said second unit EI is done based on information REF2 pertaining to an application key TA. The key is stored in rewritable non-volatile memory M.

Second unit EI can now be used and placed at a remote user location such as a gas station terminal. It should be noted that no operation key T1 has been transferred from first unit AS to second unit EI and loaded into memory M of the security modules. The operations required for both of these actions are not performed, which reduces the time needed for customization. Thus, no secret key immediately usable by an algorithm is stored, which prevents unauthorized analysis of said algorithm for uncovering said data. Consequently, it is useless for a defrauder to either spy on the communication network or the security modules in order to find out the operation key T1 used.

Another advantage of the object of the present invention lies in the fact that information SN specific to each second security unit EI is unique. Operation key T1, which has been diversified, i.e. computed based on said information, is therefore unique to each security unit EI. Therefore, encrypted application key TA, which is a function of said operation key T1, is only intended for a single second destination unit EI, which enhances the security feature of this invention. If a second unit EI does not have the same information SN as the one used for computing operation key T1 in first unit AS and if it therefore receives an application key TA which is not intended for it, it rejects this key and indicates that an error has occurred.

Other security features described below are within the scope of the present invention.

The object of the present invention provides an additional step, shown in Figure 4, according to which a random number R obtained from second unit EI is sent to first unit AS before application key TA is encrypted within first unit AS. Information that are useful, on the one hand, to encrypt application key TA in first unit AS, and on the other hand, to decrypt encrypted application key TA within second unit EI, comprise the random number obtained from second unit EI. The use of a random number R for encrypting and decrypting said application key TA avoids having the same encryption value for the same application key TA intended for a second unit EI when, for example, said key is loaded several times into said unit. Thus, each encryption of an application key TA intended for a second unit EI is unique. Therefore, a defrauder who spies on the communication network and gathers data DATA as it is transferred never obtains the same encryption value and therefore cannot uncover any secret relating to the transferred application key TA.

However, during such a transfer, the defrauder may have carried out unauthorized operations which alter the transferred data. Thus, the data DATA, which include the encrypted application key TA, are verified for integrity. For this purpose, as shown in Figure 5, a certificate CAS is computed in first unit AS on said data DATA, before said data is sent, said certificate thereafter being sent later on to the second unit EI and verified within said second unit before encrypted application key TA is decrypted in said second unit EI. In order to carry out verification, certificate CEI is computed in second unit EI based on the received data and both certificates CAS and CEI are compared. If a fraud or an error has occurred during said transfer, the verification of certificate CAS is erroneous, the decryption of application key TA is not performed and second unit EI indicates that an error has occurred. This system therefore guaranties integrity of data DATA

when it is transferred from first unit AS to second unit EI over the communication network, before using a second unit EI, that is before on-site use. Moreover, in case the verification is not valid, this avoids having to carry out an unnecessary decryption and therefore a useless waste of time.

Just as it is necessary to ensure transferred data integrity, authenticity of the data stored into second unit EI should also be guaranteed. Application key TA is thus verified for authenticity. For that purpose, as shown in Figure 5, before application key TA is encrypted, a signature SAS of said key TA is computed within first unit AS, said signature being subsequently sent to second unit EI and verified within said unit. Signature verification of said application key TA is performed after encrypted key TA is decrypted in the second unit EI and before said key within said unit is stored. In order to carry out this verification, a signature SEI is computed with the decrypted application key TA in second unit EI and the two signatures SAS and SEI are compared. When both signatures match, decrypted application key TA is authenticated and stored. In case the application key TA is not authenticated, this key is not stored and the second unit EI indicates that an error has occurred. The above-described system thus makes it possible to verify that the correct chosen application key TA has been recovered in the first unit AS and not some other key. It should be noted that when said signature SAS exists, certificate CAS is also computed as a function of said signature SAS. This signature is part of the data DATA sent during the third step described above.

Sending data such as a certificate or a signature to a security unit relies on operations whose execution time adds up to that of the customization phase. Thus, in order to reduce the number of access operations to the different units and thus, to reduce the customization time, the data set required by a security

unit is sent once by means of a single command. Random number R, number REF1 relating to an application key TA and number SN specific to second unit EI, are sent to first unit AS by means of a first single command EXPORTKEY. In the same way, encrypted application key TA, number REF2 relating to an application key TA, signature SAS, as well as certificate CAS, when they exist, are sent to second unit EI by means of a second single command IMPORTKEY.

The present invention is more particularly applicable in the case when first security unit AS is a smart card. The smart card comprises a plastic card body into which an electronic unit is embedded, which comprises an integrated circuit chip. This chip usually comprises two memories M and a third volatile memory (RAM), wherein first memory M is rewritable (EEPROM) and the second memory is not rewritable (ROM). First memory M comprises all application keys TA and transport key T. The third memory stores operation key T1. The latter only resides in said memory only during encryption or decryption of the application key in a security module. The diversification and encryption algorithms ALGO1 and ALGO2 may reside in the first or second memory M. However, it should be noted that it is not a prerequisite that these algorithms do not have to reside in the smart card. They can be stored in an entity external to said smart card, for example in a central processing unit of a terminal to which said smart card would be connected.

By means of the smart card, it is possible to ensure a better protection of application key TA. In a smart card, contrary to a computer terminal, for example, the keys are unknown to any entity (a terminal, a card administrator, another smart card, etc.) except for the entity issuing said keys. In addition, tampering is more difficult to perform on a smart card than the central processing unit of a terminal, for example. For

the same reasons, the second security unit is a smart card.

It should be noted that an application key TA, as it is stored in a non-volatile memory M, can be used on several occasions where a second unit EI is used, because even when the latter is no longer powered, the key is not erased.

CLAIMS

1. A method for customizing a set (S) of several second security units (EI), comprising secure downloading of an application key (TA) from a first security unit (AS) of a central processing unit to said set of second security units (EI), said first unit and second units each comprising at least one memory (M), characterized in that it comprises the steps of:

for each second unit (EI) in said set (S),

- on each downloading, computing an operation key (T1) in the first unit (AS) based on information specific to the second unit (EI), a transport key (T), and a diversification algorithm (ALGO1), said transport key (T) residing within the memory (M) of the first security unit (AS), said memory (M) being non-volatile,
- encrypting the application key (TA) in the first unit (AS) based on information comprising said operation key (T1) and an encryption algorithm (ALGO2), said application key (TA) residing in said memory (M),
- sending data (DATA) comprising the encrypted application key (TA) to the second unit (EI),
- on each downloading, computing an operation key (T1) in the second unit (EI) based on information specific to the second unit (EI), the transport key (T) and the diversification algorithm (ALGO1), the same transport key (T) residing in the non-volatile memory (M) of each second security unit (EI) of said set (S), said operation key (T1) not being stored within the memory (M) of said second unit,
- decrypting the encrypted application key (TA) in the second unit (EI) based on information comprising said operation key (T1) and a decryption algorithm (ALGO2P) which is the inverse of the encryption algorithm (ALGO2).

2. A method according to claim 1, characterized in that it further comprises an additional step of:

- sending information specific to the second unit (EI) to the first unit (AS) before computing the application key (T1) in the first unit (AS).

3. A method according to claims 1 or 2, characterized in that it further comprises an additional step of:

- sending a random number provided by the second unit (EI) to the first unit (AS), before encrypting the application key (TA) in the first unit (AS).

4. A method according to any of the preceding claims, characterized in that it further comprises an additional step of:

- sending information pertaining to an application key (TA) to the first unit (AS), before encrypting the application key (TA) within said unit (AS).

5. A method according to claim 4, characterized in that it further comprises an additional step of:

- choosing the application key (TA) to be encrypted based on said information.

6. A method according to any of the preceding claims, characterized in that said encryption of an application key (TA) intended for a second unit (EI) is unique.

7. A method according to any of the preceding claims, characterized in that it further comprises an additional step of:

- verifying integrity of the data (DATA) include the encrypted application key (TA).

8. A method according to any of the preceding claims, characterized in that it further comprises an additional step of:

- sending information pertaining to an application key (TA) to the second unit (EI), before decrypting the encrypted application key (TA) within said unit (EI) of said set (S).

9. A method according to any of the preceding claims, characterized in that it further comprises an additional step of:

- storing within the second unit (EI), after decrypting the encrypted application key (TA), said key (TA) within said unit (EI).

10. A method according to claim 9, characterized in that storing of the application key (TA) within the second unit (EI) is done based on information pertaining to an application key (TA).

11. A method according to any of the preceding claims, characterized in that it further comprises an additional step of:

- verifying that the application key (TA) is authentic.

12. A method according to any of the preceding claims, characterized in that the first security unit (AS) is a smart card.

13. A method according to any of the preceding claims, characterized in that the memory (M) is a rewritable memory.

14. A method according to any of the preceding claims, characterized in that a second unit (EI) comprises several application keys (TA).

15. A method according to any of the preceding claims, characterized in that the first unit (AS) comprises several application keys (TA).

16. A method according to any of the preceding claims, characterized in that it further comprises an additional step of:

- after encrypting the application key (TA), erasing the operation key (T1) temporarily saved within the second volatile memory of the first unit (AS).

17. A method according to any of the preceding claims, characterized in that it further comprises an additional step of :

- after decrypting the application key (TA), erasing the operation key (T1) temporarily saved within a second volatile memory (M2) in the first unit (EI).

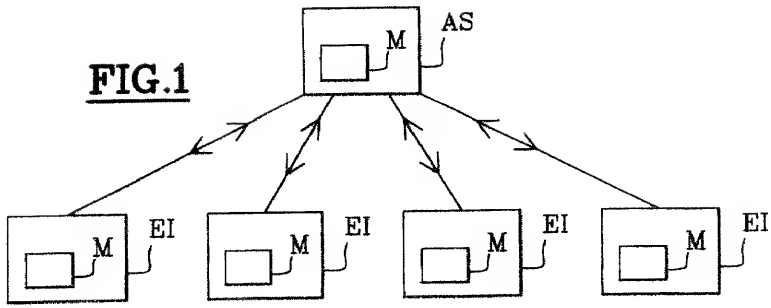
18. A method according to preceding claims 2 to 4, characterized in that it further comprises an additional step of:

- sending the random information, information (REF1) pertaining to an application key (TA) and information (SN) specific to the second unit (EI) to the first unit (AS) by means of a first single command (EXPORTKEY).

19. A method according to preceding claims 1 and 2, characterized in that it further comprises the additional steps of:

- sending the encrypted application key (TA) and the information (REF2) pertaining to an application key (TA) to the second unit (EI) by means of a single second command (IMPORTKEY).

FIG.1



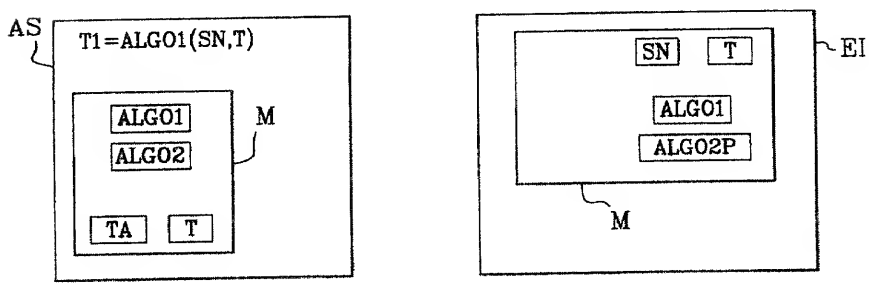


FIG.2

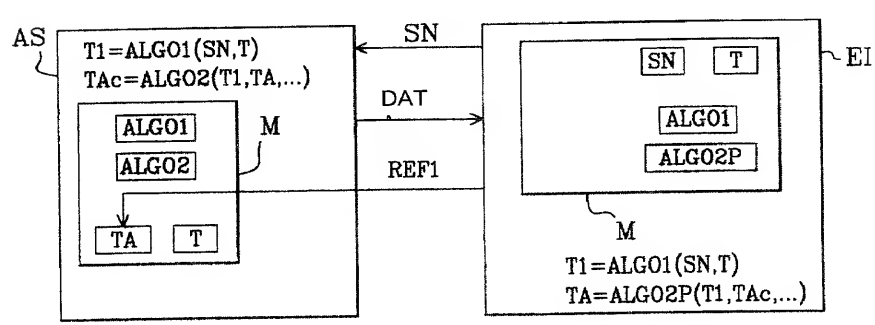


FIG.3

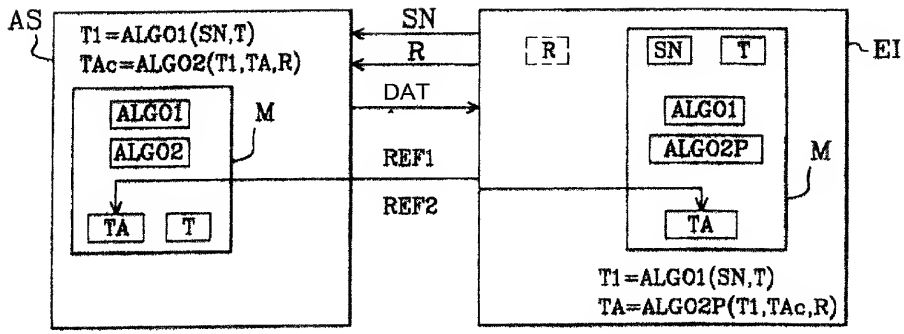

AS
T1=ALGO1(SN,T)
TAc=ALGO2(T1,TA,R)
ALGO1
ALGO2
M
TA
T
SN
R
DAT
REF1
REF2
R
SN
T
EI
ALGO1
ALGO2P
M
TA
T1=ALGO1(SN,T)
TA=ALGO2P(T1,TAc,R)

FIG.4

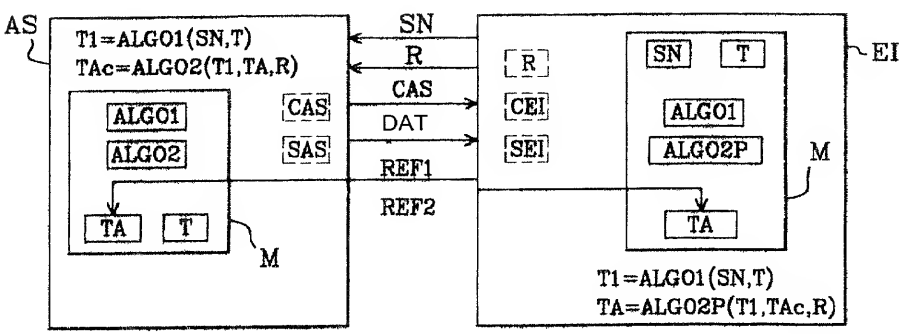

AS
T1=ALGO1(SN,T)
TAc=ALGO2(T1,TA,R)
ALGO1
ALGO2
CAS
SAS
TA
T
M
SN
R
CAS
DAT
REF1
REF2
R
CEI
SEI
SN
T
EI
ALGO1
ALGO2P
M
TA
T1=ALGO1(SN,T)
TA=ALGO2P(T1,TAc,R)

FIG.5

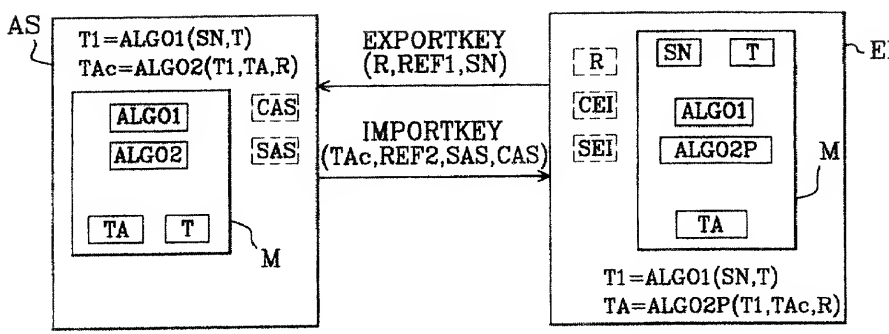

AS
T1=ALG01(SN,T)
TAc=ALG02(T1,TA,R)
ALG01
ALG02
CAS
SAS
TA
T
M
EXPORTKEY
(R,REF1,SN)
IMPORTKEY
(TAc,REF2,SAS,CAS)
R
CEI
SEI
SN
T
ALG01
ALG02P
TA
M
EI
T1=ALG01(SN,T)
TA=ALG02P(T1,TAc,R)

FIG.6

PTO/SB/01 (03-01)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

DECLARATION — Utility or Design Patent Application

Direct all correspondence to: ☐ Customer Number or Bar Code Label [ ] OR ☐ Correspondence address below

Name

Address

City | State | ZIP

Country | Telephone | Fax

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR : ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any]): 1-00 Dan | Family Name or Surname: BUTNARU

Inventor's Signature | Date: 27/02/2002

Residence: City: Yerres | State | Country: France | Citizenship: French FRX

Mailing Address: 50, Avenue Jean Jaurès – B.P. 620-12

City: Montrouge Cedex | State | ZIP: 92542 | Country: France

NAME OF SECOND INVENTOR: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any]): 2-00 Raphaël | Family Name or Surname: ROSSET

Inventor's Signature | Date: 27/02/02

Residence: City: Viroflay | State | Country: France | Citizenship: French FRX

Mailing Address: 50, Avenue Jean Jaurès – B.P. 620-12

City: Montrouge Cedex | State | ZIP: 92542 | Country: France

☒ Additional inventors are being named on the 1 supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto.

Please type a plus sign (+) inside this box →

PTO/SB/02A (11-00)
Approved for use through 10/31/2002 OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION

ADDITIONAL INVENTOR(S)
Supplemental Sheet
Page 1 of 1

Name of Additional Joint Inventor, if any:	☐ A petition has been filed for this unsigned inventor		
Given Name (first and middle [if any])	Family Name or Surname		
3rd Matthias	GELZE		
Inventor's Signature		Date 27/02/02	
Residence: City Paris	State France	Country FR	Citizenship FR
Mailing Address 50, avenue Jean Jaurès			
Mailing Address			
City Montrouge Cedex	State	ZIP 92542	Country France

Name of Additional Joint Inventor, if any:	☐ A petition has been filed for this unsigned inventor		
Given Name (first and middle [if any])	Family Name or Surname		
Inventor's Signature		Date	
Residence: City	State	Country	Citizenship
Mailing Address			
Mailing Address			
City	State	ZIP	Country

Name of Additional Joint Inventor, if any:	☐ A petition has been filed for this unsigned inventor		
Given Name (first and middle [if any])	Family Name or Surname		
Inventor's Signature		Date	
Residence: City	State	Country	Citizenship
Mailing Address			
Mailing Address			
City	State	ZIP	Country

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231

Rec'd PCT/PTO 17 DEC 2001 #4

Please type a plus sign (+) inside this box ⊞

09/889524

PTO/SB/81 (02-01)
Approved for use through 10/31/2002. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it display a valid OMB control number.

POWER OF ATTORNEY OR AUTHORIZATION OF AGENT

Application Number	09/ 889, 524
Filing Date	July 17, 2001
First Named Inventor	Dan BUTNARU
Title	Method for secure down...
Group Art Unit	
Examiner Name	
Attorney Docket Number	09669/004001

I hereby appoint:

⊞ Practitioners at Customer Number [ ] → Place Customer Number Bar Code Label here 22511 PATENT TRADEMARK OFFICE

OR

☐ Practitioner(s) named below:

Name	Registration Number

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR

☐ Practitioners at Customer Number [ ] → *Place Customer Number Bar Code Label here*

OR

☐ Firm *or* Individual Name					
Address					
Address					
City		State		Zip	
Country					
Telephone		Fax			

I am the:

⊞ Applicant/Inventor.

☐ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

SIGNATURE of Applicant or Assignee of Record

Name	Raphaël ROSSET
Signature	
Date	12/15/01

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

⊞ *Total of 2 forms are submitted.

Burden Hour Statement: This form is estimated to take 3 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Rec'd PCT/PTO 17 DEC 2001
09/889524 #4

Please type a plus sign (+) inside this box →

PTO/SB/81 (02-01)
Approved for use through 10/31/2002. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it display a valid OMB control number.

POWER OF ATTORNEY OR AUTHORIZATION OF AGENT

Application Number	09/ 889, 524
Filing Date	July 17, 2001
First Named Inventor	Dan BUTNARU
Title	Method for secure down...
Group Art Unit	
Examiner Name	
Attorney Docket Number	09669/004001

I hereby appoint:

☒ Practitioners at Customer Number [ ] →

OR

☐ Practitioner(s) named below:

Place Customer Number Bar Code Label here
22511
PATENT TRADEMARK OFFICE

Name	Registration Number

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR

☐ Practitioners at Customer Number [ ] →

OR

Place Customer Number Bar Code Label here

☐ Firm *or* Individual Name					
Address					
Address					
City		State		Zip	
Country					
Telephone		Fax			

I am the:

☒ Applicant/Inventor.

☐ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

SIGNATURE of Applicant or Assignee of Record

Name	Dan BUTNARU
Signature	
Date	12/11/2001

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 2 forms are submitted.

Burden Hour Statement: This form is estimated to take 3 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Rec'd PCT/PTO 28 FEB 2002
09/889524

Please type a plus sign (+) inside this box →

PTO/SB/81 (02-01)
Approved for use through 10/31/2002. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY OR AUTHORIZATION OF AGENT

Application Number	09/889,524
Filing Date	July 17, 2001
First Named Inventor	Dan BUTNARU
Title	Method for secure down...
Group Art Unit	
Examiner Name	
Attorney Docket Number	09069/004001

I hereby appoint:

☒ Practitioners at Customer Number [ ] → *Place Customer Number Bar Code Label here*

OR

☐ Practitioner(s) named below:

Name	Registration Number

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR

☐ Practitioners at Customer Number [ ] → *Place Customer Number Bar Code Label here*

OR

☐ Firm or Individual Name	
Address	
Address	
City	State / Zip
Country	
Telephone	Fax

I am the:

☒ Applicant/inventor.

☐ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

SIGNATURE of Applicant or Assignee of Record

Name	Matthias GELZER
Signature	
Date	27/02/02

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of [ ] forms are submitted.

Burden Hour Statement: This form is estimated to take 3 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

#1

PTO/SB/01 (03-01)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☐ Declaration Submitted with Initial Filing OR ☒ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number	09669/004001
First Named Inventor	Dan BUTNARU
COMPLETE IF KNOWN	
Application Number	09/889,524
Filing Date	July 18, 2001
Group Art Unit	
Examiner Name	

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD FOR SECURE DOWNLOADING DATA BETWEEN SECURITY UNITS.

(Title of the Invention)

the specification of which

☐ is attached hereto

OR

☒ was filed on (MM/DD/YYYY) 07/18/2001 as United States Application Number or PCT International

Application Number 09/889,524 and was amended on (MM/DD/YYYY) (if applicable).

22511
PATENT TRADEMARK OFFICE

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	Certified Copy Attached? NO
99/00462	France	01/18/1999	☐	☐	☒
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.